Listing of Claims:

This listing of claims replaces all prior versions, and listings, of claims in the application:

Claim 1. (Previously Presented) A method comprising:

receiving a request to verify a use of a digital credential by a user of a digital credential, the digital credential being a digital security mechanism associated with a user's identity, the use occurring at a first of a plurality of different services where the digital credential can be used;

verifying the use of the digital credential in response to receipt of the request to verify;

sending a result of the verification to the first service;

storing the result of the verification in an activity log in a central service that communicates with each of said plurality of different services; and

allowing specified users to access said result.

Claim 2. (Original) The method of claim 1 further including storing transaction information in the activity log.

Claim 3. (Original) The method of claim 2, wherein the transaction information includes at least one of a message that was signed using a digital signature key of the digital credential, a value of a transaction, an online service, an

internet protocol (IP) address, a date of the transaction and a time of the transaction.

Claim 4. (Original) The method of claim 1 further including generating an activity report from the activity log, wherein the activity report lists the stored verification results.

Claim 5. (Original) The method of claim 4 further including associating a name to a digital signature key of the digital credential, wherein the activity report lists the name of the digital signature key.

Claim 6. (Original) The method of claim 4, wherein generating the activity report includes generating the activity report upon request by an owner of the digital credential.

Claim 7. (Original) The method of claim 4, wherein generating the activity report includes generating the activity report each time the digital credential is verified.

Claim 8. (Original) The method of claim 4, wherein generating the activity report includes generating a report periodically.

Claim 9. (Original) The method of claim 1 further including analyzing the activity log to detect misuse of the digital credential.

Claim 10. (Original) The method of claim 6, wherein generating the activity report includes listing activity for a plurality of digital signature keys associated with the owner.

Claim 11. (Original) The method of claim 1 further comprising:

authorizing one or more delegates to use a delegated digital credential to act on behalf of the owner of the digital credential for specified functions, wherein verifying the use of the digital credential includes determining whether the delegated digital credential was authorized for the specific use.

Claim 12. (Previously Presented) The method of claim 4, wherein generating an activity report includes generating activity reports of the delegates of the user and wherein said allowing comprises allowing said user to view all reports, but allowing each said delegate to view only their own activity report, and not allowing each said delegate to view reports for other delegates.

Claim 13. (Previously Presented) An article comprising a computer-readable medium having computer-executable instructions stored thereon for causing a computer to:

receive a request to verify a use of a digital credential by a user of a digital credential at any of a plurality of different services where the digital credential can be used, the digital credential being a digital security mechanism associated with a user's identity;

verify the use of the digital credential in response to receipt of the request to verify from a first service of the plurality of different services;

send a result of the verification to the first service;

store a result of the verification in an activity log in a central service that communicates with each of said plurality of different services; and

allow specified users to access said result.

Claim 14. (Original) The article of claim 13, wherein the computer-executable instructions cause the computer to store transaction information in activity log.

Claim 15. (Original) The article of claim 14, wherein the transaction information includes at least one of a message that was signed using a digital signature key of the digital credential, a transaction value, an online service processing

the transaction, an internet protocol (IP) address of a computing device originating the transaction, the date of the transaction and the time of the transaction.

Claim 16. (Original) The article of claim 13, wherein the computer-executable instructions cause the computer to generate an activity report from the activity log, wherein the activity report lists the stored verification results.

Claim 17. (Previously Presented) The article of claim 16, wherein the computer-executable instructions cause the computer to associate a name to a digital signature key of the digital credential, wherein the activity report lists the name of the digital signature key.

Claim 18. (Previously Presented) The article of claim 16, wherein the computer-executable instructions cause the computer to generate the activity report upon receiving a request by an owner of the digital credential and wherein said allowing comprises allowing said user to view all reports, but allowing each said delegate to view only their own activity report, and not allowing each said delegate to view reports for other delegates.

Claim 19. (Original) The article of claim 13, wherein the computer-executable instructions cause the computer to analyze the activity log to detect misuse of the digital credential.

Claim 20. (Original) The article of claim 17, wherein the computer-executable instructions cause the computer to list in the activity report activity for a plurality of digital signature keys associated with the owner according to the name of the digital signature key.

Claim 21. (Original) The article of claim 20, wherein the computer-executable instructions cause the computer to authorize one or more delegates to use a delegated digital credential to act on behalf of the owner of the digital credential for specified functions and determine whether the delegated digital credential was authorized for the specific use.

Claim 22. (Original) The article of claim 21, wherein the computer-executable instructions cause the computer to generate activity reports of the delegates.

Claim 23. (Previously Presented) A system comprising:

a server to receive requests to verify digital credentials by a user of a digital credential at any of a plurality of different services where the digital credential can be used, to verify the use of the digital credential in response to receipt

of requests, and to send results from the verifications to the services;

an activity log coupled to the server to store the results from the verifications in a central service that communicates with each of said plurality of different services; and

a communication part to allow specified users to access said results.

Claim 24. (Original) The system of claim 23, wherein the activity log is configured to store transaction information for each authentication result.

Claim 25. (Original) The system of claim 24, wherein the transaction information includes at least one of a digitally signed message, a date of the transaction, a value of the transaction, an online service requesting the authentication, an internet protocol (IP) address, a value of the transaction, and a time of the transaction.

Claim 26. (Previously Presented) The system of claim 23, and further comprising an owner database to store information of an owner of the digital credential and owner-approved delegates and wherein said communication element allows said owner to view all reports, but allows each said delegate to view only their own report, and not reports for other delegates.

Claim 27. (Previously Presented) An article comprising a computer-readable medium having data structures stored thereon comprising:

a first data field to store a result from an verification of a digital credential by a user of a digital credential at any of a plurality of different services where the digital credential can be used;

a plurality of data fields to store transaction information relating to each verification result in a central service that communicates with each of said plurality of different services; and

a data access structure, allowing specified users to access said results.

Claim 28. (Original) The article of claim 27, wherein the plurality of data fields store at least one of a digitally signed message, a date of the transaction, a time of the transaction, a value of the transaction, an online service, an internet protocol (IP) address of a computing device originating the transaction, and goods or services involved in the transaction.

Claim 29. (Original) The article of claim 27, wherein the data structures further include a plurality of data fields to store owner and delegate information.

Claim 30. (Previously Presented) A method comprising:

receiving use information describing a first use of a digital credential by an owner of a digital credential, at any of a plurality of different services where the digital credential can be used, the digital credential being a digital security mechanism associated with a the owner's identity;

receiving use information describing a second use of the digital credential by a delegate of the owner of the digital credential, at any of the plurality of different services where the digital credential can be used;

storing the use information in an activity log;

generating an activity report for the delegate based on the activity log;

generating an activity report for the owner based on the activity log;

allowing said owner to view all reports; and

allowing said delegate to view only the activity report for the delegate and not the activity report for the owner or activity reports for other delegates.

Claim 31. (Original) The method of claim 30, wherein the use information includes transaction information.

Claim 32. (Original) The method of claim 30, wherein the use information includes verification information for the digital credential.

Claim 33. (Original) The method of claim 31, wherein the transaction information includes at least one of a message that was signed, a transaction value, an online service, an internet protocol (IP) address, a value of the transaction, a date of the transaction and a the time of the transaction.

Claim 34. (Original) The method of claim 30, wherein the digital credential includes a digital signature key, and further wherein generating the activity report includes associating a name to the digital signature key and listing the name of the digital signature key.

Claim 35. (Previously Presented) The method of claim 30, wherein generating the activity report for the owner includes generating the activity report upon request by an owner of the digital credential.

Claim 36. (Original) The method of claim 30, wherein generating the activity report includes generating the activity report each time the digital credential is verified.

Claim 37. (Original) The method of claim 30, wherein generating the activity report includes generating a report periodically.

Claim 38. (Original) The method of claim 30 further including analyzing the activity log to detect misuse of the digital credential.

Claim 39. (Previously Presented) The method of claim 35, wherein generating the activity report includes listing activity for a plurality of digital signature keys associated with the owner.

Claim 40. (Previously Presented) The method of claim 30 further comprising:

authorizing one or more delegates to use a delegated digital credential to act on behalf of the owner of the digital credential for specified functions, wherein verifying the use of the digital credential includes determining whether the delegated digital credential was authorized for the specific use.

Claim 41. (Previously Presented) The method of claim 30, wherein generating the activity report for the owner includes generating activity reports of the delegates of the owner.

Claim 42. (Previously Presented) A method comprising:

storing use information for a digital credential of a plurality of delegates who are delegated to use said digital credential by an owner, the digital credential being a digital security mechanism associated with the owner's identity;

processing the use information for each of said plurality of delegates to detect misuse; and

generating an alert to the owner based on the detection of misuse.

Claim 43. (Original) The method of claim 42, wherein generating an alert includes generating an activity report based on the use information.

Claim 44. (Original) The method of claim 42, wherein generating an alert includes alerting a credential service provider.

Claim 45. (Previously Presented) The method of claim 42, wherein the use information includes transaction information and wherein the method further comprises allowing said owner to view all reports, but allowing each said delegate to view only their own activity report, and not allowing each said delegate to view reports for other delegates.

Claim 46. (Original) The method of claim 42, wherein the use information includes verification information for the digital credential.

Claim 47. (Original) The method of claim 45, wherein the transaction information includes at least one of a message that was signed, a transaction value, an online service, an internet protocol (IP) address, a value of the transaction, a date of the transaction and a the time of the transaction.

Claim 48. (Previously Presented) A method comprising:

receiving transaction requests from a plurality of delegate users who are delegated from an owner, wherein the transaction requests include digital credentials for the delegate users, the digital credentials being digital security mechanisms associated with users' identities;

processing the transaction requests; and

communicating transaction information to a central service, wherein the transaction information includes the digital credentials of the delegates, the transaction information communicated to create, for the plurality of delegate users, activity reports regarding the usage of the digital credentials, the activity reports created at the central service that said owner is allowed to view while each delegate is allowed to view

only their own activity report and not allowed to view reports for other delegates.

Claim 49. (Original) The method of claim 48, wherein processing the transaction requests includes communicating the digital credentials to the central service for verification.

Claim 50. (Previously Presented) The method of claim 48, wherein processing a requested transaction includes:

verifying the digital credential; and

communicating a result of the verification to the credential service.

Claim 51. (Original) The method of claim 48 further including receiving a activity report from the central service, wherein the activity report lists the transaction information for each digital credential.

Claim 52. (Original) The method of claim 48, wherein the transaction information includes at least one of a message that was signed, a transaction value, an online service, an internet protocol (IP) address, a value of the transaction, a date of the transaction and a the time of the transaction.

Claim 53. (Previously Presented) A method comprising:

receiving a request from a medical professional to access

medical information at a remote service, wherein the request includes a digital credential for the medical professional, the digital credential being a digital security mechanism associated with the medical professional's identity;

communicating transaction information describing the access request and the digital credential to a credential verification service;

receiving a verification result from the credential verification service;

providing the medical professional access to the medical information based on the verification result; and

receiving an activity report from the credential verification service, wherein the activity report lists the transaction information, the digital credential and the transaction result.

Claim 54. (Original) The method of claim 53, wherein the transaction information includes at least an access type, a date of the transaction and a time of the transaction.

Claim 55. (Original) The method of claim 53, further wherein the digital credential was provided by a credential issuing service and a credential service provider.

Claim 56. (Original) The method of claim 53, and further including:

receiving a request to access the activity report from an owner of the digital credential; and

providing the owner access to the activity report.